Protocol melding en afhandeling beveiligings- of datalek

Versie 4 juni 2018

1. Inleiding

De achtergrond van deze procedure is de Meldplicht datalekken. Met ingang van 1 januari 2016 is de Wet bescherming persoonsgegevens ('Wbp') aangevuld met artikel 34a Wbp. Sindsdien geldt een meldplicht voor datalekken. Ook in de komende Algemene Verordening Gegevensbescherming ('AVG') is een dergelijke meldplicht voor datalekken opgenomen. Deze meldplicht houdt in dat organisaties een datalek onverwijld moeten melden aan de Autoriteit Persoonsgegevens (AP) (en in bepaalde gevallen ook aan de betrokkenen).

Dit document beschrijft de procedure die gehanteerd wordt bij (het vermoeden van) een beveiligings- of datalek binnen Factorium Cultuurmakers, dan wel bij (het vermoeden van) een beveiligings- of datalek dat buiten Factorium Cultuurmakers heeft plaatsgevonden maar waarvoor Factorium Cultuurmakers toch de verantwoordelijkheid draagt (bij een 'verwerker'). Deze procedure is mede gebaseerd op de 'Beleidsregels voor de toepassing van artikel 34a van de Wbp' ('Beleidsregels') van de AP.

Beveiligings- of datalekken zijn incidenten rondom verwerkingen van persoonsgegevens met een potentieel grote impact. Als Factorium Cultuurmakers als gevolg van een datalek een grote groep betrokkenen moet informeren kan dit grote kosten met zich meebrengen. Het snel en adequaat onderzoeken, beperken van de gevolgen, het melden en afhandelen van een datalek zijn dan ook van groot belang.

Met het volgen van deze procedure wordt het volgende resultaat nagestreefd:

- voorspelbaar zijn voor alle belanghebbenden;
- waarborgen van de belangen van Factorium Cultuurmakers en de betrokkenen;
- op systematische wijze analyseren van een (mogelijk) beveiligings- of datalek;
- het nemen van passende verbetermaatregelen en het structureel borgen ervan.

Leeswijzer en onderhoud

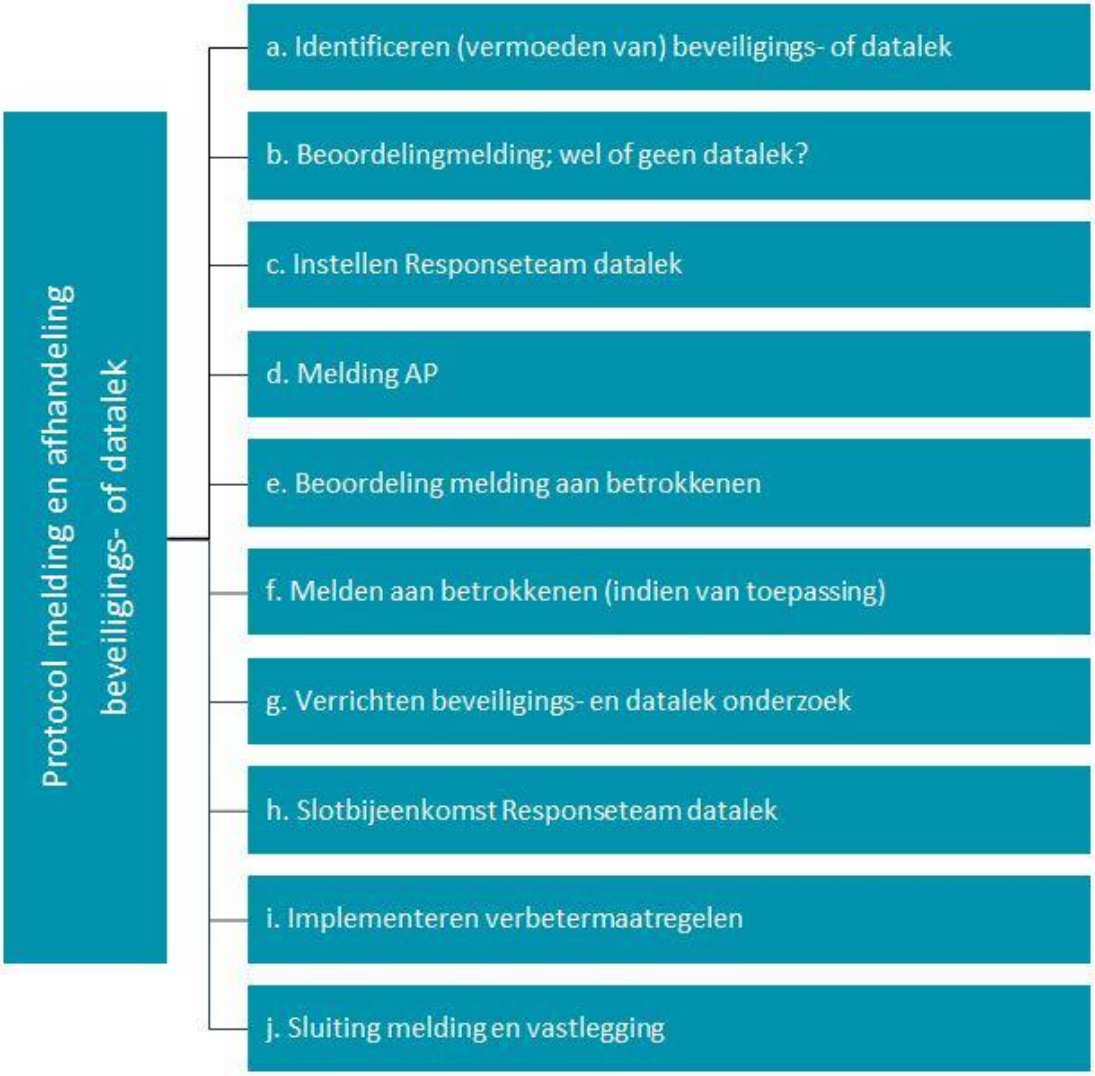
De activiteiten in het protocol, bijbehorende verantwoordelijkheden en bevoegdheden worden in de volgende paragrafen stapsgewijs uitgewerkt.

2. Definities

Betrokkene:	degene op wie een persoonsgegeven betrekking heeft
Datalek:	een inbreuk op de beveiliging waarbij persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking; dus blootgesteld aan datgene waartegen beveiligingsmaatregelen bescherming hadden moeten bieden.

Eigenaar:	persoon die namens Factorium Cultuurmakers de gedelegeerde verantwoordelijkheid heeft voor een informatiemiddel & -verwerkingen.
PG:	Porteuillehouder Gegevensbescherming.
Beveiligingslek:	een mogelijk beveiligingslek, waardoor de bescherming van persoonsgegevens op enig moment is doorbroken en waardoor de persoonsgegevens mogelijk zijn blootgesteld aan verlies of onrechtmatige verwerking. Het is daarbij niet van belang of de verantwoordelijke passende technische of organisatorische beschermingsmaatregelen heeft getroffen of niet. Ieder datalek is een beveiligingslek, niet ieder beveiligingslek is een datalek.
Persoonsgegevens:	alle gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd.
Verwerker	degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
Verwerking van persoonsgegevens:	een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens zoals bijvoorbeeld het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
(Verwerkings-)verantwoordelijke:	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. In dit geval Factorium Cultuurmakers.
Wet	Wet bescherming persoonsgegevens (“Wbp”) en Algemene Verordening Gegevensbescherming (“AVG”).

3. Protocol



a. Identificeren van een beveiligings- of datalek

De melding van (een vermoeden) van een beveiligings- of datalek kan te allen tijde door iedereen worden gedaan, door personeelsleden Factorium Cultuurmakers, maar ook door externen binnen en buiten Factorium Cultuurmakers. Eenieder die een (mogelijk) beveiligings- of datalek constateert, meldt dit incident per omgaande bij de PG via pg@factorium.nl

b. Beoordeling melding; wel of geen datalek?

De PG neemt op verzoek of eigen initiatief contact op met de melder (mits de melding niet anoniem is gedaan). De PG zorgt zo spoedig mogelijk voor volledige en juiste informatie, zoals opgenomen in het meldingsformulier van AP (autoriteit persoonsgegevens) en zorgen voor een eerste analyse om te bekijken of er sprake is van een beveiligings- of datalek.

De beoordeling of er sprake is van een beveiligings- of datalek, en of er gemeld moet

worden aan AP, komt tot stand met behulp van de (beslisbomen uit) Beleidsregels. Bij de beoordeling spelen o.a. een rol:

- is er enkel sprake van een dreiging van verlies (dus een beveiligingslek)?
- is er sprake van verlies van persoonsgegevens;
- is er sprake van onrechtmatige verwerking van persoonsgegevens;
- is er sprake van een enkele tekortkoming of kwetsbaarheid in de beveiliging;
- kan redelijkerwijs worden uitgesloten dat een inbreuk op de beveiliging tot een onrechtmatige verwerking heeft geleid;
- zijn er persoonsgegevens van gevoelige aard gelekt;
- leiden de aard en de omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen.

In geval dat het beveiligingslek niet heeft geleid tot verlies of onrechtmatige verwerking van persoonsgegevens is er geen sprake van een datalek, maar van een beveiligingslek. Melding bij AP is dan niet aan de orde, maar de melding wordt dan wel geregistreerd door de PG en gerapporteerd aan de directie.

c. Instellen Responseteam datalek

Het team bestaat uit de PG en de directeur/bestuurder en de betrokken verantwoordelijke voor ICT.

Het responsteam draagt zorgt voor:

- beoordeling van de melding;
- uitvoering noodzakelijke acties met betrekking tot het datalek (bijvoorbeeld datalek onmiddellijk dichten, sporen verzamelen, toegang tot informatie beperken en eventueel hulp inroepen voor nader onderzoek);
- of en wat gemeld gaat worden bij AP;
- wijze van afhandeling intern,
- of er sprake is van eigen aansprakelijkheid, of aansprakelijkheid van derden;
- het al dan niet doen van aangifte en vaststellen of er sprake is van strafrechtelijke verwijtbaarheid;
- besluiten over in-en externe communicatie
- of eventuele schade is gedekt door de verzekeringspolis.

d. Melding AP

De PG verzorgt tijdig de elektronische melding bij AP . De PG registreert de ontvangstbevestiging van AP en slaat het meldingsformulier op. De contactpersoon AP fungeert inzake de communicatie met AP.

e. Beoordeling melding aan betrokkenen

Indien een datalek is gemeld aan AP, dient tevens vastgesteld te worden of het datalek ook moeten worden gemeld aan degenen om wiens gegevens het gaat (betrokkenen) met behulp van de schema's uit de Beleidsregels.

f. Melden aan betrokkenen (indien van toepassing)

In opdracht van de directie stelt de PG in samenspraak met de directeur een kennisgeving aan betrokkenen op.
De melding bevat in ieder geval de aard van de inbreuk, contactgegevens Factorium Cultuurmakers, het informatiepunt waar de betrokkenen meer informatie over de inbreuk kan krijgen en de maatregelen die Factorium Cultuurmakers de betrokkenen aanbeveelt om te nemen teneinde de negatieve gevolgen van de inbreuk te beperken.

g. Verrichten datalek onderzoek

De PG onderzoekt of en zo ja hoe dergelijke datalekken in de toekomst voorkomen kunnen worden.

De bevoegdheden van het responsteam zijn:

- vrijheid om met alle partijen betrokken bij het datalek en de melding te spreken;
- alle relevant geachte documenten & data inzien en bewaren;
- toegang tot alle plaatsen die het team nodig acht ten behoeve van een zorgvuldige analyse;
- actie naar verwerkers conform afspraken in de toepasselijke verwerkersovereenkomst;
- het recht en de middelen om externe deskundigen in te zetten in het onderzoek.

De directie besluit daarop:

- welke verbetermaatregelen getroffen moeten worden;
- of en hoe over het rapport en de aanbevelingen gecommuniceerd wordt.

h. Implementeren verbetermaatregelen

De eigenaar van het betrokken informatiemiddel of -verwerking is ook verantwoordelijk voor de implementatie van de vanuit het beveiligings- of datalek vastgestelde verbetermaatregelen. Hij ziet toe op de communicatie rondom de verbetermaatregelen en dat de genomen maatregelen worden geëvalueerd op effectiviteit. Hij rapporteert over de voortgang van deze stappen aan de directeur.

i. Sluiting melding en vastlegging

De PG informeert het responsteam, de directie en de direct bij het incident betrokken personen op het moment dat het datalek definitief afgehandeld is en de melding gesloten is. Het datalek wordt opgenomen in de registratie bij de PG.